CLAIMS

1. An apparatus for automatically detecting unwanted messages in real time in a system that includes a message server for routing incoming message files to a directory, the apparatus comprising:

a redundant email address detection and capture system (READACS), said READACS comprising a computer implemented program comprising:

a process for accessing said directory and for identifying said message files;

a process for locating any of an address-of-origin, subject, or other specified criteria within each said message file;

a process for identifying whether each said message file should be considered spam;

a process for separating said spam and non-spam message files logically; and

a process for any of physically moving and renaming said message files in a predetermined fashion.

2. The apparatus of Claim 1, wherein said process for identifying whether each said message file should be considered spam applies any of a frequency threshold and a quantity threshold.

3. The apparatus of Claim 1, said READACS further comprising a process for identifying message files that are excepted from said process for identifying whether each said message file should be considered spam.

4. A method for automatically detecting unwanted messages in real time in a system that includes a message server for routing incoming message files to a directory, the method comprising the steps of:

accessing said directory and for identifying said message files;

locating any of an address-of-origin, subject, or other specified criteria within each said message file;

identifying whether each said message file should be considered spam;

separating said spam and non-spam message files logically; and

any of physically moving and renaming said message files in a predetermined fashion.

5. The method of Claim 4, wherein said identifying whether each said message file should be considered spam step applies any of a frequency threshold and a quantity threshold.

6. The method of Claim 4, further comprising the step of:

identifying message files that are excepted from said identifying whether each said message file should be considered spam step.

7. The method of Claim 4, said accessing step further comprising the steps of:

reading a RecentFileList from a RecentFile; and

loading said RecentFileList into a RecentListArray;

wherein if a BypassFileList is included, reading said BypassFileList into a BypassArray.

8. The method of Claim 7, said locating step further comprising the steps of:

creating a NewListArray;

opening said message files;

extracting message addresses of a sender as defined in any of MailInDirName, AddrLineLocator, and AddrInfoLocator fields;

loading said NewListArray with new message sender addresses and associated file names.

9. The method of Claim 8, said locating step further comprising the steps of:

setting an arrival time for all records in said NewListArray;

combining said NewListArray into said RecentListArray;

marking new records as IsNew = True; and'

sorting said RecentListArray by message sender addresses.

10. The method of Claim 9, said identifying step further comprising the steps of:

determining the age of a message sender address based upon a SecondsThreshold when a message sender address is retrieved from said RecentListArray;

if said message file is older than said threshold, marking said message file as IsExpired = True by Seconds Threshold;

determining whether said message sender address occurs more often than a SourceThreshold allows;

optionally, if yes, examining said message sender address to determine if it is to be passed anyway because it is identified in said BypassArray; and

marking said message file as IsSpam = True if said message file exceeds said SourceThreshold, and said SecondThreshold has not timed out, and optionally said message file is not listed in said BypassArray.

11. A method for automatically detecting unwanted messages in real time in a system that includes a message server for routing incoming message files to a directory, the method comprising the steps of:

receiving a message file at a host system;

routing said message file to said directory;

writing said message file with a prefix and/or suffix that allows it to be identified as a new message;

identifying all message files in said directory that are spam; and

any of renaming and moving said message files.

12. The method of Claim 11, wherein a message file is identified as spam based upon said message file's address-of-origin, where said address-of-origin is identified by a process comprising the steps of:

identifying a line on which a message file address may reside; and

extracting said address-of-origin from said line by searching for an indicator within said line.

13. The method of Claim 11, wherein message files are analyzed and determined to be spam or non-spam through a combination of a time threshold, bypass exceptions and tolerances, and a maximum number of allowed messages from any one address

14. The method of Claim 11, said method requiring minimum implementation parameters which comprise:

a path and/or name of a recent file;

a path and/or name of a bypass file;

an incoming mail directory;

a directory and/or file name suffix for non-spam mail;

a directory and/or file name suffix for spam mail;

a number of seconds to accumulate information before clearing it;

a number of occurrences of any one address to allow within a value; and

a string for which to search within each file processed to determine if said string should contain an address; wherein only a first occurrence of a locator within a file is evaluated.

15. The method of Claim 11, said method implementation parameters optionally comprising:

partial file names to be excluded from processing; wherein any file including a specific string specified is excluded from processing;

partial file names to be included in processing; wherein only files including a string specified are processed;

a suffix for processed non-spam files (SetRenameSuffix); only optional if SetDestinationDirName is defined.

a destination directory path for non-spam files;

a suffix for processed spam files;

a destination directory path for spam files; and

a string defining what should be considered an address within a line previously identified.

16 An apparatus for redundant email address detection and capture, comprising:

a plurality of sending entities for originating email messages;

a public network for routing said email messages to a destination;

a destination mail server;

a mechanism at said mail server for identifying newly arrived messages;

a directory to which are newly arrived messages re routed; and

a mechanism for examining messages in said directory and for classifying said messages as spam or non-spam based upon a number of messages received from an identified sending address within a specific interval;

wherein non-spam messages are routed to appropriate destinations in accordance with previously established routing instructions; and

wherein spam is sent to one or more predetermined destinations.